REMARKS/ARGUMENTS

In response to the non-final Office Action dated February 18, 2010, Applicants respectfully request reconsideration and allowance of the instant application based upon the amendment and arguments presented herein. Claims 2-7, 9, 12-17 and 19 have been amended to be in a more preferred form. Additionally, the specification has been amended to cure minor informalities. No new matter has been introduced. Claims 2-10 and 12-20 remain pending in this application.

Rejections under 35 U.S.C. § 103

Claims 2-10 and 12-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent no. 5,132,992 to Yurt et al ("Yurt") in view of U.S. patent no. 5,999,629 to Heer et al. ("Heer"). Applicants respectfully traverse these rejections.

Independent claim 12 recites, among other features, the following:

> the remote server configured to store in storage a video program encrypted in a first encrypted form received from at least one programming source which is located remote from the remote server,

The Office Action relies on Yurt for these features. Yurt is deficient for at least the following reasons. First, Yurt does not receive a video program encrypted in a first encrypted form "from at least one programming source which is located remote from the remote server," as recited by claim 12. In support of this rejection, the Office Action, at page 6, quotes Yurt, col. 6, ll. 35-39, which states, "Prior to being made accessible to a user of the transmission and receiving system of the present invention, the item must be stored in at least one compressed data library 118, and given a unique identification code by [the] identification encoder." Thus, the Office Action characterizes Yurt's "compressed data library 118" as allegedly describing a "programming source which is located remote from the remote server" and Yurt's "transmission system 100" as allegedly describing the remote server of claim 12. However, even assuming, without admitting, that the transmission system of Yurt is equivalent to a remote server, the compressed data library of Yurt is not "located remote from the remote server," as recited by claim 12. Indeed, Yurt explicitly states that the compressed data library is part of the transmission system:

> Further, according to the present invention, the transmission system preferably includes compressed data library means for separately storing composite formatted data blocks for each of the files. The compressed data storage means preferably includes compressed data library **118**, as shown in FIG. 2*b*. After the data is processed into a file by the compressed data storage means **117**, it is preferably stored in a compressed data library **118**. In a preferred embodiment, compressed data library **118** is a network of mass storage devices connected together via a high speed network. Access to any of the files stored in compressed data library **118** is available from multiple reception systems **200** connected to the transmission and receiving system.

Yurt, col. 10, ll. 31-45.

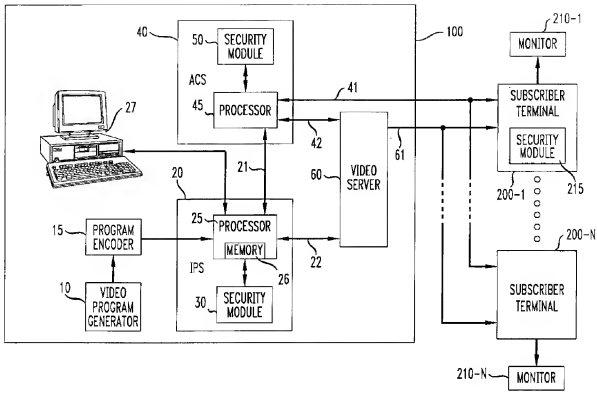
Therefore, Yurt does not teach or suggest "the remote server configured to store in storage a video program…received from at least one programming source which is located remote from the remote server," as recited by claim 12. Second, Yurt does not contemplate encryption. Indeed, Yurt describes a system that only performs data compression. *See, e.g.,* Yurt, col. 2, ll. 25 – col. 3, ll. 15. Compression does not teach or suggest encryption. *See, e.g.,* Heer, col. 2, ll. 35-65 (describing a video delivery system that first compresses data then supplies the compressed data to a *separate* security module for encryption). Thus, it follows, that Yurt does not teach or suggest "the remote server configured to store in storage a video program encrypted in a first encrypted form," as recited by claim 12. Heer is cited for other features and does not teach or suggest a modification to Yurt that would overcome these noted deficiencies of Yurt.

Additionally, independent claim 12 recites, among other features, the following:

> the remote server configured to process the decrypted video program to produce a video program in a second encrypted form; and
> the remote server configured to transmit the video program in the second encrypted form to the requesting user.

The Office Action correctly notes that Yurt fails to teach or suggest these features. Instead, the Office Action relies on Heer for these features. Specifically, the Office Action at page 7 quotes Heer at col. 5, ll. 59-62 and col. 7, ll. 17-18 as describing these features. Heer at col. 5, ll. 59-62 states, "module 50 unloads the module 30/50 symmetrical key CV from memory and decrypts the encrypted program encryption key using CV. Module 50 then re-encrypts the program encryption key using its device unique key." Heer at col. 7, ll. 17-18 states "Processor 45 then transmits the message over bus 41 for distribution to the subscriber terminals 200i." The above cited portions of Heer do not relate to a "remote server configured to process the decrypted video program to produce a video program in a second encrypted form," as recited in claim 12. Instead, the above cited portions of Heer merely describe encrypting an encryption key.

Indeed, Heer fails to teach or suggest producing "a video program in a second encrypted form," as recited in claim 12. For example, Heer describes a system that includes a plurality of security modules that are used to "maintain the secrecy of the intelligence that may be used by computers to communicate with another, for example, by encrypting the messages that they exchange with one another." Heer, abstract; *see also,* Heer, Fig. 1. However, these security modules are not utilized in Heer "to produce a video program in a second encrypted form," as recited by claim 12. With reference to Heer's Fig. 1, the illustrated embodiment includes three security modules: security module 30, security module 50, and security module:



Heer, Fig. 1

Security module 30 is the only module that encrypts the program. Specifically, security module 30 encrypts information "using a unique program encryption key that head-end security module 30 [previously] generated for that purpose." Heer, col. 2, ll. 48-51. Notably, it is this video server that transmits the program to the terminal. *See, e.g.,* Heer, col. 7, ll. 40-65. The remaining encryption processes of Heer relate to encryption of the program encryption key and not the video program. For example, security module 50 and security module 30 communicate an encrypted version of the program encryption key using a key shared only by security modules 50 and 30. *See, e.g.,* Heer, col. 5, ll. 55-61. Similarly, security module 50 and security module 215 communicate an encrypted version of the program encryption key using a key shared only by security modules 50 and 215. *See, e.g.,* Heer, col. 6, ll. 20-36. Thus, even assuming, without admitting, that the video delivery system of Heer is equivalent to a remote server, Heer does not teach or suggest "the remote server configured to process the decrypted video program to produce a video program in a second encrypted form," as recited in claim 12. Additionally,

because Heer does not teach or suggest "the remote server configured to process the decrypted video program to produce a video program in a second encrypted form," Heer also does not teach or suggest "the remote server configured to transmit the video program in the second encrypted form to the requesting user," as recited by claim 12.

Accordingly, for at least these reasons, Yurt and Heer, alone or in any combination thereof, fail to teach or suggest the features of independent claim 1. Thus, independent claim 1 distinguishes over the art of record and is in condition for allowance.

Independent claim 13, although different in scope, recites language substantially similar to that of independent claim 12 and distinguishes over the cited documents for at least the same reasons as discussed above with respect to claim 12.

Dependent claims 2-10 and 14-20 depend from one of independent claims 12 and 13, and distinguish over the cited documents for the same reasons as their base independent claim, and further in view of the novel and non-obvious features recited therein.

For example, claim 8 recites, among other features, the following: "wherein the video program in the second encrypted form is encrypted according to a Data Encryption Standard (DES)." The Office Action at page 5 relies on Heer's "DES processor" for these features. However, in Heer, "DES" stands for "Digital Encryption System." Heer, col. 8, line 67. A "Digital Encryption System" does not teach or suggest a "video program in the second encrypted form is encrypted according to a Data Encryption Standard (DES)," as recited by claim 8.

Claim 18 recites similar language to claim 8 and is similarly distinguishable.

As another example, claim 9 recites, among other features, the following: "the remote server is adapted to multiplex the video program in the second encrypted form and other signals to create a multiplexed signal for transmission to the requesting user." The Office Action at page 5 relies on Heer's multibit multiplexer as describing this feature. However, the multibit multiplexer is merely a digital component of the security module's "input data handler" that includes such common digital components as a "register, byte counter and a multibit, e.g., 32 bit, multiplexer." As explicitly stated in Heer, the input data handler "receives byte-wide data from a so-called transport chip and formats the data into 32 bit words for either processor 2 or output data handler 14" of Fig. 5. Heer, col. 9, line 63 – col. 10, line 2. Thus, Heer's multibit

multiplexer does not teach or suggest "the remote server is adapted to multiplex the video program in the second encrypted form and other signals to create a multiplexed signal for transmission to the requesting user," as recited by claim 9.

Claim 19 recites similar language as claim 9 and is similarly distinguishable.

CONCLUSION

It is believed that no fee is required for this submission. If any fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit our Deposit Account No. 19-0733, accordingly.

All rejections having been addressed, applicants respectfully submit that the instant application is in condition for allowance, and respectfully solicit prompt notification of the same.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: May 18, 2010

By: /Evan M. Clark/
Evan M. Clark
Registration No. 64,836

1100 13th Street, N.W., Suite 1200
Washington, D.C. 20005-4051
Tel: (202) 824-3000
Fax: (202) 824-3001